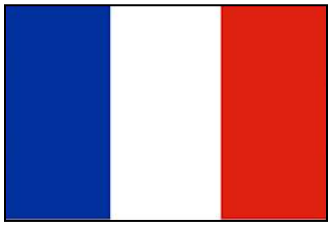
Cyber Security Opportunities in France

FRANCE
Capital: Paris
Population: 66.6 million
GDP: US $2.8 trillion
Currency: EURO
Language: French



Summary

The French cybersecurity market is highly advanced in terms of the expertise and capacity of local industry professionals. Furthermore, recent incidences such as enterprise level cyberattacks and international cyberwarfare have increased awareness of cybersecurity threats and have bolstered demand for cybersecurity products in the country. The need for enhanced security solutions remains critical for a wide range of Information technology sectors, including business analytics; mobile computing; cloud computing; and social media. Automotive systems' susceptibility to hacking also remains a concern. In addition, new potential targets worth noting include industrial systems (future factories) as well as the budding e-payment sector. Moreover, the increased use of the Internet as a principal medium of communication in the public and private sector as well as the fast growing usage of connected devices (including smart phones but also a plethora of other objects, such as automobiles) have greatly increased cyber vulnerabilities. It is expected that 15% of all objects will have internet connectivity come the year 2020. Overall, cybercrime's cost to French companies exceeded €3.3 billion in the year 2015, with the theft of banking data and patents representing half the number of total incidents. Faced with a wide range of concerns, French authorities and enterprises are intent on dealing with cyber terrorism and cyber warfare through the design of more sophisticated hardware and software solutions.

Undoubtedly, the French cybersecurity sector is one of considerable dynamism. An increase in concern over recent high-level cyber intrusions (such as the costly attack suffered by the global television network TV5 Monde in 2015) as well as a strong demand for homegrown cybersecurity solutions have combined to bolster the local market. At present, a limited number of companies, almost exclusively French, command a dominant market share. In fact, in 2014, the top five companies in the French market (Morpho, Thales, Orange, Cassidian and Atos) represented over 75% of total sales. Despite the top-heavy structure of the market, an emergence of smaller startup firms offering creative solutions is thought to potentially bring about greater levels of fragmentation. Currently filling 40,000 jobs, the French cybersecurity industry is expected to grow at a rate of 10% per year and reach €2 billion in size in 2017.

New drivers in France to improve consciousness and industrial response include:

1.) From 2014 to 2019, the French government, in an effort to become a truly global power in the matter, has committed to invest €1 billion in its national cyber defense. A 2013 White Paper published under Francois Hollande has reaffirmed this commitment to cyber security. The paper specifically highlights the need for cybersecurity solutions to accompany the massive increase in digital infrastructure experienced in France. It is important to note as well that the government seems intent on supporting the cyber security sector as a matter of national security, especially following the string of terrorist attacks France has experienced over the course of the last two years.

2.) Starting on August 2014, ANSSI (France's national cybersecurity agency) has drafted a series of documents and prepared a working group in order to delineate a practical approach to strengthen the cybersecurity of France's industrial infrastructure. ANSSI is also developing a security label for cloud operators in order to aid businesses in better distinguishing secure cloud support services, a service which should fortify confidence in the technology. Partly as a result of ANSSI's leadership, the number of cyberattacks experienced in France has been decreasing. Per a study published by PwC, French businesses experienced 47% less cyberattacks in 2016 than the preceding year.

3.) Since July 2016, an expansion of a 2013 law (la Loi de Programmation Militaire), has taken into effect, mandating that a wide swath of organizations and businesses (250 in total) whose operations are deemed "essential to the nation" take measures to actively protect their information systems. More decrees of a similar nature are expected to follow.

Market Demand

The French IT-Security market consists of three key segments: small to medium-sized businesses, large corporations, and the French government; which includes civil, security, military, and critical national infrastructures (e.g. utilities and telecoms). Cyber threats to such organizations can only be addressed through the design of solutions that integrate hardware, software, and services. The movement towards networked IT infrastructures and other innovative technologies such as the Internet of Things, the Cloud and Smart Cities will drive further demand for cybersecurity products designed to alleviate potential vulnerabilities inherent in these highly integrated technologies.

Software solutions stand as the principal portion of the cyber-security market, with anti-viruses, firewalls and other tracking devices being installed in businesses of all types and sizes. This sector is one of the fastest-growing segments of the French software industry. Within the security hardware sector, companies are looking after standard Unified Threat Management (UTM) appliances that make it possible for solutions to be adopted on a large scale at an affordable cost. The French government is intent on developing cross-border collaboration among EU members so that powerful hardware solutions can be made available on a global scale.

Best Prospects

Security Software: Software as a Service (SaaS); anti-virus software; content-management software; Security for mobile environment; Security for Cloud Computing IT outsourcing; Security Information and Event Management (SIEM); Cryptography software, Identity and Access Management solutions; software associated with disclosure regulations.

Security Services: Managed Information Security Services (MISS); outsourcing; security audits and penetration testing; services associated with compliance and disclosure regulations, Software system & Insurance package combination; risk analysis;

Security Appliances: Unified Threat Management (UTM) - the unification of firewall, VPN, ID&P systems and gateway antivirus into a single platform; wireless and application security solutions; biometric technology.

Prospective Buyers

It is important to note that striking deals with entities whose IT security is deemed critical to the nation (e.g. major financial institutions, transportation companies, utilities, and governmental bodies such as the Ministries of Interior and Defense; the Ministries of finances and health care, the office for Immigration and Border Protection; the French IRS and Customs) will more likely than not be out of reach for all except the largest of American cybersecurity players. Instead, companies deemed less essential to the state, and those that are generally smaller in size, would represent more realistic targets for American companies.

Market Entry

Selling through an established local French partner represents the best market entry strategy for most U.S. firms, especially when the Partner is a software integrator with solid contacts in the country. There may be exceptions when selling to French government entities, where a direct business presence in France is required for issues related to national security.

Market Issues and Obstacles

France's IT security market is open and a number of U.S. firms already operate successfully in France. However, there are specific French regulations American firms seeking to enter this market should be aware of. These include: the Data Protection Act, Privacy and electronic communication, The Freedom of Information Act, Environmental issues and European regulations. Most public sector procurement contracts in France above a minimum value threshold are subject to formal EU procurement procedures. For small businesses hoping to compete for government contracts, this can create a significant challenge, given the level of resources often required to respond to very detailed public sector tender notices. Another notable obstacle that should be noted is the very low level of trust in U.S. service providers that exists in the French market. This tension has only been strengthened over the last decade by controversies such as the Patriot Act and recent NSA activities.

Resources and Events

France Cyber Security Strategy: http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cybersecurite/

French success in cybersecurity sphere: https://www.challenges.fr/challenges-soir/moitie-moins-de-cyber-attaques-en-france_434127

About the Loi de Programmation Militaire: http://www.lefigaro.fr/secteur/high-tech/2016/06/28/32001-20160628ARTFIG00229-les-entreprises-strategiques-sommees-de-renforcer-leur-protection-informatique.php

Industry's response to cyber-threats: http://www.cf2r.org/fr/tribunes-libres/l-entreprise-face-aux-cybermenaces.php

For cyber news – see http://www.usinenouvelle.com/article/cybersecurite-l-arme-secrete-du-made-in-france.N187051

Contact Information

Name:	Charles DeFranchi
Email:	charles.defranchi@trade.gov
Phone:	+33 14 31 27 163

Name: Christophe Joly
Email: christophe.joly@trade.gov
Phone: +33 14 31 27 003

Updated: Feb. 2017

The U.S. Commercial Service — Your Global Business Partner With its network of offices across the United States and in more than 80 countries, the U.S. Commercial Service of the U.S. Department of Commerce utilizes its global presence and international marketing expertise to help U.S. companies sell their products and services worldwide. Locate the U.S. Commercial Service trade specialist in the U.S. nearest you by visiting http://www.export.gov/.

Disclaimer: The information provided in this report is intended to be of assistance to U.S. exporters. While we make every effort to ensure its accuracy, neither the United States government nor any of its employees make any representation as to the accuracy or completeness of information in this or any other United States government document. Readers are advised to independently verify any information prior to reliance thereon. The information provided in this report does not constitute legal advice.